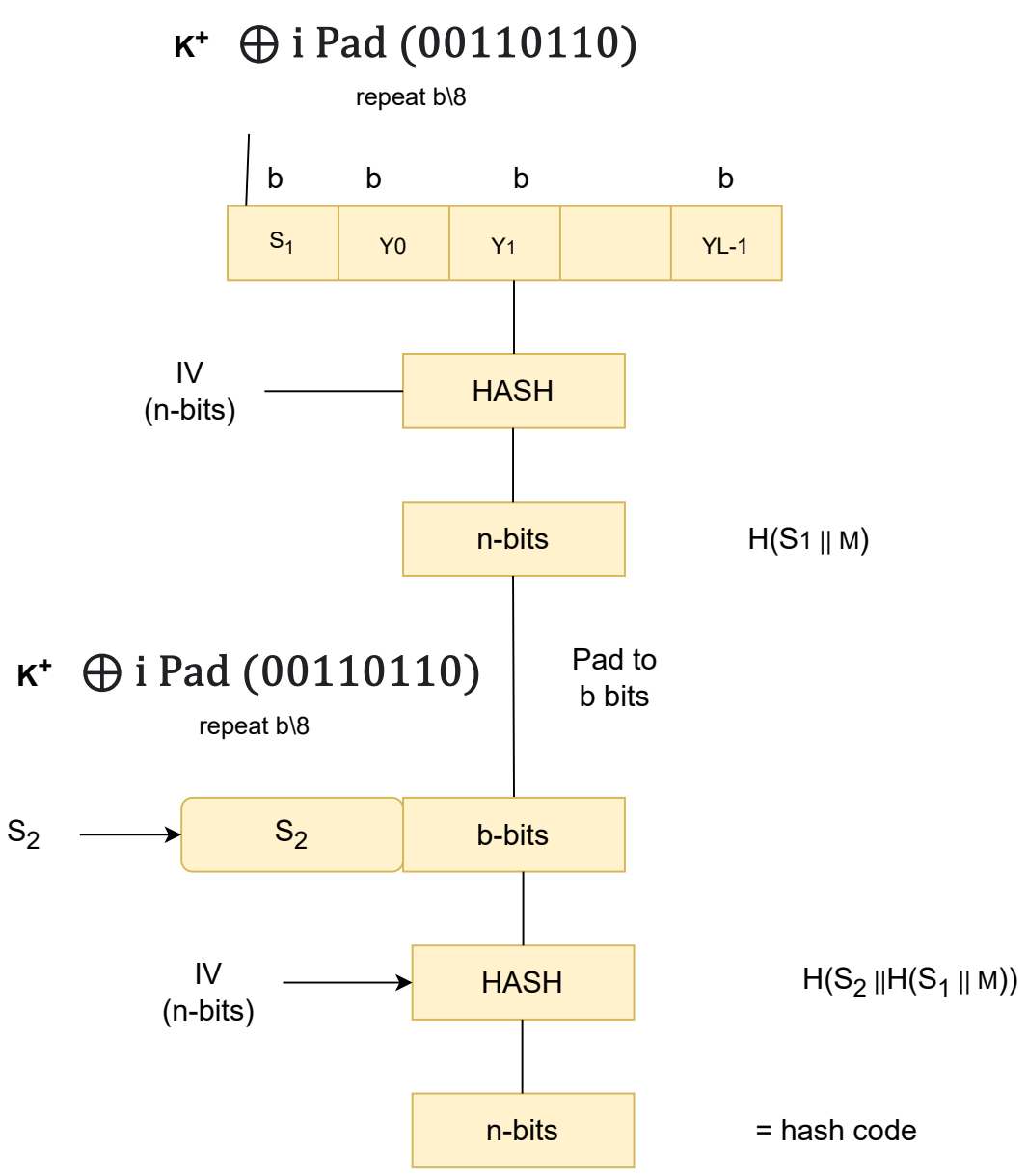
K+ ⊕ i Pad (00110110)
repeat b\8
b
b
b
b
S1
Y0
Y1
YL-1
IV
(n-bits)
HASH
n-bits
H(S1 || M)
K+ ⊕ i Pad (00110110)
repeat b\8
Pad to
b bits
S2
S2
b-bits
IV
(n-bits)
HASH
H(S2 ||H(S1 || M))
n-bits
= hash code